

1 Kaveh S. Elihu, Esq. (SBN 268249)
2 Saima Ali Gipson, Esq. (SBN 324752)
3 **EMPLOYEE JUSTICE LEGAL GROUP, PC**
4 1001 Wilshire Boulevard
5 Los Angeles, California 90017
6 Telephone: (213) 382-2222
7 Facsimile: (213) 382-2230
8 Email: kelihu@ejlglaw.com
9 sali@ejlglaw.com

10 Attorneys for Plaintiff,
11 Iran Carranza

12 UNITED STATES DISTRICT COURT
13 CENTRAL DISTRICT OF CALIFORNIA

14 IRAN CARRANZA, an
15 individually, and on behalf of all
16 similarly situated individuals,

17 Plaintiff,

18 v.

19 TICKETMASTER LLC., a
20 Virginia Limited Liability
21 Company; and DOES 1 through 50,
22 inclusive,

23 Defendants.

Case No.

24 **CLASS ACTION COMPLAINT**
25 **JURY TRIAL DEMANDED**

26 Plaintiff Iran Carranza (“Plaintiff”) individually and on behalf of all other
27 similarly situated, brings this action against Defendant Ticketmaster LLC.
28 (“Defendant”) based on personal knowledge and the investigation of counsel, and
allege as follows:

INTRODUCTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the
harms caused to Plaintiff and other similarly situated persons (“Class” or “Class
Members” or “Breach Victims”) in a massive and preventable data breach of
Defendant’s inadequately protected cloud database.

1 2. Defendant revealed in a June 28, 2024 notification to the Maine
2 Attorney General that a hacker gained unauthorized access to Defendant's cloud
3 database, owned and operated by Snowflake, Inc., information on April 2, 2024 (the
4 "Data Breach" or "Breach").

5 3. Defendant did not discover the Data Breach until May 23, 2024, nearly
6 seven weeks later.

7 4. Defendant did not notify Plaintiff or the Breach Victims until July 17,
8 2024, another almost two months after the Data Breach was discovered.

9 5. Further, Defendant determined that the Data Breach contained sensitive
10 personal information ("Personal Information"), including names, basic contact
11 information, and payment card information such as encrypted credit or debit card
12 numbers and their expiration dates of Plaintiff and Breach Victims.

13 6. The Personal Information of 560 million consumers, including
14 Plaintiff, was affected by this Data Breach.¹

15 7. The hackers, known as ShinyHunters, posted the data of the 560
16 million consumers on an illicit online marketplace for sale for \$500,000.²

17 8. In short, thanks to Defendant's failure to protect the Breach Victims'
18 Personal Information, cybercriminals were able to steal everything they could
19 possibly need to commit nearly every conceivable form of identity theft and wreak
20 havoc on the financial and personal lives of hundreds of millions of individuals.

21 9. Defendant is an American ticket sales and distribution company based
22 in Beverly Hills, California and incorporated in Virginia.

23 10. Defendant's conduct – failing to implement adequate and reasonable
24 measures to ensure their electronic systems were protected, failing to take adequate
25

26 ¹ [https://cybernews.com/news/ticketmaster-notifies-customers-omits-important-
27 details/#:~:text=Ticketmaster%20has%20finally%20contacted%20its%20customers
28 %20regarding%20a,involved.%20The%20scope%20of%20compromised%20informa-
tion%20remains%20unknown.](https://cybernews.com/news/ticketmaster-notifies-customers-omits-important-details/#:~:text=Ticketmaster%20has%20finally%20contacted%20its%20customers%20regarding%20a,involved.%20The%20scope%20of%20compromised%20information%20remains%20unknown.)

² *Id.*

1 steps to prevent and stop the Data breach, and failing to timely detect the breach,
2 failing to disclose the material facts that they did not have adequate electronic
3 systems and security practices to safeguard the Personal Information, failing to
4 honor their duty to protect the Breach Victims' Personal Identities, and failing to
5 provide timely and adequate notice of the Data Breach – caused substantial harm
6 and injuries to Plaintiff and the Breach Victims.

7 11.As a result of the Data Brach, Plaintiff and the Breach Victims have
8 suffered damages. Now that their Personal Information has been hacked, Plaintiff
9 and Breach Victims are at imminent risk of identity theft. And this will continue, as
10 they must spend their time being extra vigilant, due to Defendant's failures, to try to
11 prevent being victimized for the rest of their lives.

12 12.Plaintiff brings this class action lawsuit on behalf of a nationwide and
13 statewide class to hold Defendant responsible for its negligent and reckless failure to
14 use reasonable, current cybersecurity measures to protect class members' Personal
15 Information.

16 13.Because Defendant presented such a soft target to cybercriminals,
17 Plaintiff and Breach Victims have already been subjected to violations of their
18 privacy, fraud, and identity theft, or have been exposed to a heightened and
19 imminent risk of fraud and identity theft. Plaintiff and Breach Victims must now
20 and in the future, spend time to more closely monitor their credit reports, financial
21 accounts, phone lists, and online accounts to guard against identity theft.

22 14.Plaintiff and Breach Victims may also incur out-of-pocket costs for,
23 among other things, purchasing credit monitoring services, credit freezes, credit
24 reports, or other protective measures to deter and detect identify theft.

25 15.On behalf of herself and the Breach Victims, Plaintiff seeks actual
26 damages, statutory damages, and punitive damages, with attorney fees, costs, and
27 expenses under negligence, negligence per se, breach of fiduciary duties, breach of
28

1 confidence, breach of implied contract, and invasion of privacy. Plaintiff also seeks
2 injunctive relief, including significant improvements to Defendant's data security
3 systems, future annual audits, and long-term credit monitoring services funded by
4 Defendant, and other remedies as the Court sees fit.

5 **THE PARTIES**

6 11.Plaintiff Iran Carranza is a citizen of California, currently residing in
7 Los Angeles, California.

8 12.Defendant Ticketmaster LLC. is a Virginia limited liability company
9 based in Beverly Hills, California.

10 13.The true names and capacities of persons or entities, whether
11 individual, corporate, associate, or otherwise, who may be responsible for some of
12 the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek
13 leave of court to amend this Complaint to reflect their true names and capacities of
14 such other responsible parties when their identities become known.

15 14.All of Plaintiff's claims stated herein are asserted against Defendant
16 and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

17 **JURISDICTION AND VENUE**

18 15.Plaintiff incorporates by reference all allegations of the preceding
19 paragraphs as though fully set forth herein.

20 16.Defendant is a Virginia limited liability company with its principal
21 place of business in Beverly Hills, California.

22 17.Jurisdiction is proper under 28 U.S.C. § 1332(d)(2) because Plaintiff
23 seeks relief on behalf of a Nationwide Class, which will result in at least one class
24 member belonging to a different state than that of Defendant.

25 18.Additionally, Plaintiff is seeking damages for a nationwide and
26 statewide Class that will exceed the \$5,000,000.00 threshold for federal court
27 jurisdiction. Therefore, both diversity jurisdiction and the damages threshold under
28

1 the Class Action Fairness Act of 2005 (“CAFA”) are present, and this Court has
2 jurisdiction.

3 19. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because
4 Defendant operates, resides and has its principal place of business in this district,
5 and a substantial part of the events or omissions giving rise to the claims occurred in
6 this district.

7 **FACTUAL ALLEGATIONS**

8 20. Plaintiff incorporates by reference all allegations of the preceding
9 paragraphs as though fully set forth herein.

10 21. On June 28, 2024, Defendant submitted a notice with the Office of the
11 Attorney General in Maine (“Maine Notice”) that a Data Breach occurred that
12 resulted in the theft of sensitive information on April 2, 2024, but was not
13 discovered until May 23, 2023.³

14 22. Defendant also reported in the Maine Notice that 63,206 persons were
15 affected by this Data Breach nationwide.

16 23. On July 17, 2024, Defendant sent letters to Plaintiff and other Breach
17 Victims informing them that, it detected an unauthorized user had gained access to
18 their electronic systems on April 2, 2024 (“Notice of Breach” or “Notice”). The
19 Notice also informed Plaintiff and Breach Victim that Defendant conducted a
20 review of the relevant file that was involved in the Breach and determined that the
21 file may include Plaintiff’s and Breach Victim’s Personal Information. However,
22 Defendant was not transparent in its notice regarding the extent of personal
23 information that was stolen from its cloud database. Defendant has admitted that the
24 breach contained names and credit or debit card numbers, including expiration
25 dates. However, what they failed to disclose in its Notice is that Breach Victim’s

26 _____
27 ³ Data Breach Notifications, Office of the Maine Attorney General,
28 <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/0d26b6dd-b466-4f2a-bec0-ec2ad0738583.html>

1 breached Personal Information includes not just names, but also social security
2 numbers, dates of birth, physical addresses, telephone numbers, driver's license
3 information, payroll information, financial account information, and other
4 confidential personal data.⁴

5 24.Despite detecting the breach in April 2024, and knowing that Plaintiff
6 and Class Members were in danger, Defendant did nothing to warn Breach Victims
7 until another nearly two months later. During this time, the cyber criminals had free
8 reign to surveil and defraud their unsuspecting victims. Indeed, the cyber criminals
9 already posted Class Members' stolen data online on May 27, 2024 for \$500,000 in
10 sales.

11 25.In spite of the severity of the Data Breach, Defendant has done very
12 little to protect Breach Victims. Defendant is only offering one year of credit
13 monitoring protection services.

14 26.Defendant failed to adequately safeguard Breach Victims' Personal
15 Information, allowing cyber criminals to access this wealth of priceless information
16 for months before Defendant warned the Breach Victims to be on the lookout.

17 27.Defendant had an obligation created by reasonable industry standards,
18 common law, and its representations to Breach Victims, to keep their Personal
19 Information confidential and to protect the information from unauthorized access.

20 28.Plaintiff and Breach Victims provided their Personal Information to
21 Defendant with the reasonable expectations and mutual understanding that
22 Defendant would comply with its obligations to keep such information confidential
23 and secure from unauthorized access.

24
25
26
27 ⁴ Zach Whittaker, *Live Nation confirms Ticketmaster was hacked, says personal*
28 *information stolen in data breach*, <http://techcrunch.com/2024/05/31/live-nation-confirms-ticketmaster-was-hacked-says-personal-information-stolen-in-data-breach>.

1 29. Because the Data Breach was an intentional hack by cyber criminals
2 seeking information of value that they could exploit, Breach Victims are at
3 imminent risk of severe identity theft and exploitation.

4 30. Plaintiff is very careful about not sharing her sensitive Personal
5 Information. She has never knowingly transmitted unencrypted sensitive Personal
6 Information over the internet or any other unsecured source.

7 31. Plaintiff stores any document containing her Personal Information in
8 safe and secure locations or destroys such documents.

9 32. Since the Data Breach, Plaintiff has received an influx of spam
10 telephone calls and messages.

11 33. Plaintiff has suffered imminent and impending injury arising from the
12 substantially increased risk of fraud, identity theft, and misuse resulting from her
13 Personal Information, especially her Social Security number, being placed in the
14 hands of unauthorized third parties and possibly criminals.

15 34. Plaintiff has a continuing interest in ensuring that her Personal
16 Information, which, upon information and belief, remains backed up in Defendant's
17 possession, is protected and safeguarded from future breaches.

18 35. Defendant collects, maintains, and stores the Personal Information of
19 Plaintiff and the Breach Victims in the usual course of business.

20 36. In addition to its obligations under federal and state laws, Defendant
21 owed a duty to its consumers, the Breach Victims whose Personal Information was
22 entrusted to Defendant to exercise reasonable care in obtaining, retaining, securing,
23 safeguarding, deleting, and protecting the Personal Information in its possession
24 from being compromised, lost stolen, accessed, and misused by unauthorized
25 persons. Defendant owed a duty to Plaintiff and Breach Victims to provide
26 reasonable security, including consistency with industry standards and requirements,
27 and to ensure that its electronic systems and networks, and the personnel responsible
28

1 for them, adequately protected the Personal Information of the Plaintiff and Breach
2 Victims.

3 37.Further, Defendant had a duty to train its personnel in exercising
4 reasonable care in obtaining, retaining, securing, safeguarding, deleting, and
5 protecting the Personal Information of other employees.

6 38.Defendant owed a duty to Plaintiff and the Breach Victims whose
7 Personal Information was entrusted to Defendant to design, maintain, and test its
8 computer and electronic systems and email systems to ensure that Personal
9 Information in Defendant's possession was adequately secured and protected.

10 39.Defendant owed a duty to Plaintiff and the Breach Victims whose
11 Personal Information was entrusted to Defendant to create and implement
12 reasonable data security practices and procedures to protect the Personal
13 Information in their possession, including adequately training its employees and
14 others who accessed Personal Information within its computer systems on how to
15 adequately protect Personal Information.

16 40.Defendant owed a duty to Plaintiff and the Breach Victims whose
17 Personal Information was entrusted to Defendant to implement processes that would
18 detect a breach on its data security systems in a timely manner.

19 41.Defendant owed a duty to Plaintiff and the Breach Victims whose
20 Personal Information was entrusted to Defendant to act upon data security warnings
21 and alerts in a timely fashion.

22 42.Defendant owed a duty to Plaintiff and the Breach Victims whose
23 Personal Information was entrusted to Defendant to disclose if its computer systems
24 and data security practices were inadequate to safeguard individuals' Personal
25 Information from theft because such an inadequacy would be a material fact in the
26 decision to entrust Personal Information with Defendant.

1 43. Defendant owed a duty to Plaintiff and the Breach Victims whose
2 Personal Information was entrusted to Defendant to disclose in a timely and accurate
3 manner when data breaches occurred.

4 44. Defendant owed a duty of care to Plaintiff and the Breach Victims
5 because they were foreseeable and probable victims of any inadequate data security
6 practices.

7 45. Defendant knew or should have known that Defendant's computer
8 and/or electronic systems were a target for cybersecurity attacks because warnings
9 were readily available and accessible via the Internet.

10 46. Each year, identity theft causes tens of billions of dollars of losses to
11 victims in the United States.⁵ Cyber criminals can leverage Plaintiff's and Breach
12 Victims' Personal Information that was stolen in the Data Breach to commit
13 numerous additional crimes, including opening new financial accounts in Breach
14 Victims' names, taking out loans in Breach Victims' names, using Breach Victims'
15 names to obtain government benefits, using Breach Victims' Personal Information
16 to file fraudulent tax returns using Breach Victims' information, obtaining driver's
17 licenses in Breach Victims' names but with another person's photograph, and
18 giving false information to police during an arrest. Even worse, Breach Victims
19 could be arrested for crimes identity thieves have committed.

20 47. Personal Information is like currency today. It is an extremely valuable
21 commodity to identify thieves that once the information has been compromised,
22 criminals often trade the information on the cyber black-market for years.

23 48. Today, a person's personal information can be worth more than \$1,000
24 on the dark web. Online banking login information costs on average \$100, and
25
26

27 ⁵ Facts + Statistics: Identity Theft and Cybercrime, Insurance Info. Inst., [https://www.iii.org/fact-statistic/facts-](https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime)
28 statistics-identity-theft-and-cybercrime

1 \$150 if the bank account has a minimum of \$100 in the account.⁶ Full credit card
2 details and associated data costs between \$10 and \$100.⁷ A high-Hackquality US
3 driver's license with stolen identity information on it costs about \$500.⁸ A full
4 range of documents and information on a person that will allow identity theft can
5 be purchased for about \$1,000.⁹

6 49. Based on the foregoing, the information compromised in the Data
7 Breach is significantly more valuable than the loss of, for example, credit card
8 information in a retailer data breach, because, there victims can cancel or close
9 credit and debit card accounts. The information compromised in this Data Breach
10 is impossible to "close" and difficult, if not impossible, to change.

11 50. This Data Breach has and will lead to further devastating financial and
12 personal losses to Breach Victims.

13 51. This is not speculative, as the Federal Trade Commission has reported
14 that if hackers get access to Personal Information, they *will* use it.¹⁰

15 52. Plaintiff and the Breach Victims have experienced one or more of these
16 harms as a result of the Data Breach.

17 53. As described above, identity theft victims must spend countless hours
18 and large amounts of money repairing the impact to their credit.¹¹

19 54. Defendant's offer of one year of credit monitoring to Plaintiff and the
20 Breach Victims is woefully inadequate. While some harm has begun already, the
21

22 ⁶ Smith, Ryan, Revealed – how much is personal information worth on the dark web, Insurance Business (May 1,
23 2023), <https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx#:~:text=An%20individual's%20personal%20information%20can,by%20cybersecurity%20researcher%20Privacy%20Affairs.>

24 ⁷ *Id.*

25 ⁸ *Id.*

26 ⁹ *Id.*

27 ¹⁰ Lazarus, Ari, How fast will identity thieves use stolen info?, Military Consumer (May 24, 2017),
<https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info>

28 ¹¹ "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013),
<http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf>.

1 worst may be yet to come. There may be a time lag between when harm occurs
2 versus when it is discovered, and also between when Personal Information is stolen
3 and when it is used. Furthermore, credit monitoring only alerts someone to the fact
4 that they have already been the victim of identity theft (i.e. fraudulent acquisition
5 and use of another person's Personal Information)—it does not prevent identity
6 theft.

7 55. As a direct and proximate result of the Data Breach, Plaintiff and the
8 Breach Victims have been placed at an imminent, immediate, and continuing
9 increased risk of harm from fraud and identity theft. Plaintiff and the Breach
10 Victims now have to take the time and effort to mitigate the actual and potential
11 impact of the Data Breach on their everyday lives, including placing “freezes” and
12 “alerts” with credit reporting agencies, contacting their financial institutions,
13 closing or modifying financial accounts, and closely reviewing and monitoring
14 bank accounts and credit reports for unauthorized activity for years to come.

15 56. Plaintiff and the Breach Victims have suffered, and continue to suffer,
16 actual harms for which they are entitled to compensation, including:

- 17 i. Trespass, damage to and theft of their personal property
18 including Personal Information;
 - 19 ii. Improper disclosure of their Personal Information;
 - 20 iii. The imminent and certainly impending injury flowing from
21 potential fraud and identity theft posed by their Personal
22 Information being placed in the hands of criminals and having
23 been already misused;
 - 24 iv. Damages flowing from Defendant untimely and inadequate
25 notification of the data breach;
 - 26 v. Loss of privacy suffered as a result of the data breach;
- 27
28

- vi. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;
- vii. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market;
- viii. The loss of use of and access to their credit, accounts, and/or funds;
- ix. Damage to their credit due to fraudulent use of their Personal Information; and
- x. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

57. Moreover, Plaintiff and Breach Victims have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

58. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Breach Victims one year of credit monitoring services. One year of credit monitoring is woefully inadequate to protect Plaintiff and Breach Victims from a lifetime of identity theft risk and does nothing to reimburse Plaintiff and Breach Victims for the injuries they have already suffered.

CLASS ALLEGATIONS

59. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

60. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23 (a) and 23(b)(3), Plaintiff asserts all claims on behalf of a Nationwide Class, as defined as follows: **All persons whose Personal Information was compromised by the**

April 2, 2024 Data Breach at Ticketmaster, including all who were sent a notice of the Data Breach.

61.Excluded from the Class is Defendant, its legal representatives, assignees, and successors, and any entity in which the Defendant has controlling interest. Also, excluded from the Class is the judge to whom this case is assigned, the Judge’s immediate family, and Plaintiff’s counsel and their employees. Plaintiff reserves the right to amend the above-stated class definitions based on facts learned in discovery, as well as adding subclasses as the Court sees fit.

62.Alternatively, Plaintiff Proposes the following subclasses by state or groups of states, defined as follows: **Statewide [Name of State] Class: All residents of [name of State] whose Personal Information was compromised by the April 2, 2024 Data Breach at Ticketmaster.**

63.The proposed Nationwide Class, or alternatively, the separate Statewide Class (collectively, the “Class” as used in this sub-section) meet the requirements under Rule of Civil Procedure 23 (a), (b)(1), (b)(2), (b)(3), and (c)(4).

64.**Numerosity:** The proposed Class is so numerous that joinder all members is impracticable.

65.**Commonality and Predominance:** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual Class Members. These common legal and factual questions include, but are not limited to, the following:

- xi. Whether Defendant failed to adequately safeguard Plaintiff’s and the Class’s Personal Information;
- xii. Whether Defendant failed to protect Plaintiff’s and the Class’s Personal Information;
- xiii. Whether Defendant’s email and computer systems and data security practices used to protect Plaintiff’s and the Class’s

- 1 Personal Information violated federal and state laws, and/or
2 Defendant's other duties;
- 3 xiv. Whether Defendant violated the data security statutes and data
4 breach notification statutes applicable to Plaintiff and the Class;
- 5 xv. Whether Defendant failed to notify Plaintiff and members of the
6 Class about the Data Breach expeditiously and without
7 unreasonable delay after the Data Breach was discovered;
- 8 xvi. Whether Defendant engaged in unfair, unlawful, or deceptive
9 practices by failing to safeguard Breach Victims' Personal
10 Information properly and as promised;
- 11 xvii. Whether Defendant acted negligently in failing to safeguard
12 Plaintiff's and the Class's Personal Information;
- 13 xviii. Whether Defendant entered into implied contracts with Plaintiff
14 and the members of the Class that included contract terms
15 requiring Defendant to protect the confidentiality of Personal
16 Information and have reasonable security measures;
- 17 xix. Whether Defendant violated the consumer protection statutes,
18 data breach notification statutes, and state privacy statutes
19 applicable to Plaintiff and the Class;
- 20 xx. Whether Defendant failed to notify Plaintiff and Breach Victims
21 about the Data Breach as soon as practical and without delay
22 after the Data Breach was discovered;
- 23 xxi. Whether Defendant's conduct described herein constitutes a
24 breach of their implied contracts with Plaintiff and the Class;
- 25 xxii. Whether Plaintiff and the members of the Class are entitled to
26 damages as a result of Defendant's wrongful conduct;
- 27
28

xxiii. What equitable relief is appropriate to redress Defendant's wrongful conduct; and

xxiv. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Class.

66. **Typicality:** Plaintiff's claims are typical of the Class and within each subclass and are based on the same facts, legal theories and/or primary rights of all Class members, because Plaintiff and each Class member were identically injured in by having their Personal Information accessed by unauthorized persons as a direct result of Defendant's Data Breach.

67. **Superiority:** The class action procedure is also superior to individual lawsuits due to the massive volume of potential individual lawsuits and the similarities that persist in each Class member's claims when compared against the predicted amount of recovery per Class member. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if members of the Class could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

68. **Adequacy:** Plaintiff will adequately and fairly protect the interests of the Class. She has retained counsel experiences in class action litigation. Neither Plaintiff nor her counsel have any interest that might cause them to not vigorously pursue this action in the Class's best interest.

69. Plaintiff and her counsel anticipate that notice to the proposed Class will be effectuated by mailing notice to each and every individual that Defendant

1 has already sent a Notice regarding the Data Breach to on or around July 17, 2024,
2 whose Personal Information was potentially accessed by unauthorized users during
3 the Data Breach.

4 70. This case is appropriate for certification because prosecution of
5 separate actions would risk either inconsistent adjudications which would establish
6 incompatible standards of conduct for the Defendant or would be dispositive of the
7 interests of members of the proposed Class. Furthermore, Defendant are still in
8 possession of Personal Information of Plaintiff and the Class, and Defendant's
9 systems are still vulnerable to attack—one standard of conduct is needed to ensure
10 the future safety of Personal Information in Defendant's possession.

11 71. This case is appropriate for certification because Defendant has acted
12 or refused to act on grounds generally applicable to Plaintiff and the Class as a
13 whole, thereby requiring the Court's imposition of uniform relief to ensure
14 compatible standards of conduct towards members of the Class, and making final
15 injunctive relief appropriate with respect to the proposed Class as a whole.
16 Defendant's practices challenged herein apply to and affect the members of the
17 Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's
18 conduct with respect to the proposed Class as a whole, not on individual facts or law
19 applicable only to Plaintiff.

20 **FIRST CAUSE OF ACTION**

21 ***(Negligence – By Plaintiff on behalf of the Class, against Defendant and***
22 ***Does 1-50)***

23 72. Plaintiff incorporates by reference all allegations of the preceding
24 paragraphs as though fully set forth herein.

25 73. Defendant solicited, gathered, and stored the Personal Information of
26 Plaintiff and the Class.

74. Defendant knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiff and the Class and the importance of adequate security.

75. Defendant were well aware of the fact that hackers routinely attempted to access Personal Information without authorization. Defendant also knew about numerous, well-publicized data breaches wherein hackers stole the Personal Information from companies, including its own company, who held or stored such information.

76. Defendant owed duties of care to Plaintiff and the Class whose Personal Information was entrusted to it. Defendant's duties included the following:

- i. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Personal Information in its possession;
- ii. To protect the Personal Information in its possession using reasonable and adequate security procedures and systems;
- iii. To adequately and properly train its employees to avoid phishing emails;
- iv. To use adequate email security systems, including DMARC enforcement and Sender Policy Framework enforcement, to protect against phishing emails;
- v. To adequately and properly train its employees regarding how to properly and securely transmit and store Personal Information;
- vi. To train its employees not to store Personal Information in their email inboxes longer than absolutely necessary for the specific purpose that it was sent or received;
- vii. To implement processes to quickly detect a data breach, security incident, or intrusion; and

viii. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Personal Information.

77. Because Defendant knew that a security incident, breach or intrusion upon its systems would potentially damage thousands of its current and/or former consumers, including Plaintiff and Class members, it had a duty to adequately protect their Personal Information.

78. Defendant owed a duty of care not to subject Plaintiff and the Class to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices

79. Defendant knew, or should have known, that its security practices and computer systems did not adequately safeguard the Personal Information of Plaintiff and the Class. Defendant breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and security practices to safeguard the Personal Information of Plaintiff and the Class.

80. Defendant breached their duties of care by failing to provide prompt notice of the Data Breach to the persons whose personal information was compromised.

81. Defendant acted with reckless disregard for the security of the Personal Information of Plaintiff and the Class because Defendant knew or should have known that their computer systems and data security practices were not adequate to safeguard the Personal Information that it collected and stored, which hackers were attempting to access.

82. Defendant acted with reckless disregard for the rights of Plaintiff and the Class by failing to provide prompt and adequate notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use of Personal Information compromised in the Data Breach.

83. Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and the Class's willingness to entrust Defendant with their personal information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to choose a provider to store its extensive database of consumers' Personal Information that would properly safeguard and monitor against such data breaches.

84. Defendant own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Personal Information. Defendant's misconduct included failing to:

- ix. Comply with current industry standard security practices;
- x. Encrypt Personal Information during transit and while stored on Defendant's systems;
- xi. Develop a written records retention policy that identifies what information must be kept and for how long;
- xii. Employ or contract with trained professionals to ensure security of network servers and evaluate the systems used, and so forth;
- xiii. Avoid using Social Security numbers as a form of identification; and
- xiv. Have a plan ready and in position to act quickly should a theft or data breach occur.

85. Defendant also had independent duties under federal and state law requiring them to reasonably safeguard Plaintiff's and the Class's Personal Information and promptly notify them about the Data Breach.

86. Defendant breached the duties they owed to Plaintiff and Class members in numerous ways, including:

- xv. By creating a foreseeable risk of harm through the misconduct previously described;

- 1 xvi. By failing to implement adequate security systems, protocols and
2 practices sufficient to protect their Personal Information both
3 before and after learning of the Data Breach;
4 xvii. By failing to comply with the minimum industry data security
5 standards before, during, and after the period of the Data Breach;
6 and
7 xviii. By failing to timely and accurately disclose that the Personal
8 Information of Plaintiff and the Class had been improperly
9 acquired or accessed in the Data Breach.

10 87. But for Defendant wrongful and negligent breach of the duties it owed
11 Plaintiff and the Class members, their Personal Information either would not have
12 been compromised or they would have been able to prevent some or all of their
13 damages.

14 88. As a direct and proximate result of Defendant's negligent conduct,
15 Plaintiff and the Class have suffered damages and are at imminent risk of further
16 harm.

17 89. The injury and harm that Plaintiff and Class members suffered (as
18 alleged above) was reasonably foreseeable.

19 90. The injury and harm that Plaintiff and Class members suffered (as
20 alleged above) was the direct and proximate result of Defendant's negligent
21 conduct.

22 91. Plaintiff and the Class have suffered injury and are entitled to damages
23 in an amount to be proven at trial.

24 ///

25 ///

26 ///

27 ///

SECOND CAUSE OF ACTION

(Negligence Per Se – *By Plaintiff on behalf of the Class, against Defendant and Does 1-50*)

92. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

93. Pursuant to the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the Personal Information of Plaintiff and the Class.

94. The FTCA prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also formed part of the basis of Defendant’s duty in this regard.

95. Defendant solicited, gathered, and stored the Personal Information of Plaintiff and the Class as part of its business of selling tickets to entertainment events nationwide, which affects commerce.

96. Defendant violated the FTCA by failing to use reasonable measures to protect the Personal Information of Plaintiff and the Class and not complying with applicable industry standards, as described herein.

97. Defendant breached its duties to Plaintiff and the Class under the FTCA and other state data security and privacy statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Breach Victim’s Personal Information.

98. Defendant’s failure to comply with applicable laws and regulations constitutes negligence per se.

99. Plaintiff and the Class are within the class of persons that the FTCA was intended to protect.

100. The harm that occurred as a result of the Data Breach is the type of harm the FTCA, the state data breach privacy statutes were intended to guard against.

101. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate network systems and data security practices to safeguard Plaintiff's and the Class's Personal Information.

102. Defendant breached their duties to Plaintiff and the Class by negligently and unreasonably delaying and failing to provide notice expeditiously and/or as soon as practicable to Plaintiff and the Class of the Data Breach.

103. Defendant's violation of the FTCA, state data security statutes, and/or the state data breach notification statutes constitute negligence per se.

104. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach by, inter alia, having to spend time reviewing their accounts and credit reports for unauthorized activity; spend time and incur costs to place and re-new a "freeze" on their credit; be inconvenienced by the credit freeze, which requires them to spend extra time unfreezing their account with each credit bureau any time they want to make use of their own credit; and becoming a victim of identity theft, which may cause damage to their credit and ability to obtain insurance, medical care, and jobs.

105. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

///

///

///

///

THIRD CAUSE OF ACTION

(Breach of Fiduciary Duties– *By Plaintiff on behalf of the Class, against Defendant and Does 1-50*)

106. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

107. A relationship existed between Plaintiff and Class Members and Defendant in which Plaintiff and the Class put their trust in Defendant to protect their Personal Information. Defendant accepted this duty and obligation when it received Plaintiff and the Class Members' Personal Information.

108. Plaintiff and the Class Members entrusted their Personal Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Personal Information for business purposes only, and refrain from disclosing their Personal Information to unauthorized third parties.

109. Defendant knew or should have known that the failure to exercise due care in the collecting, storing, and using of individual's Personal Information involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

110. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff and the Class's information in Defendant's possession was adequately secured and protected.

111. Defendants also had a fiduciary duty to have procedures in place to detect and prevent improper access and misuse of Plaintiff's and the Class's

1 Personal Information. Defendant's duty to use reasonable security measures arose
2 as a result of the special relationship that existed between Defendant and Plaintiff
3 and the Class. That special relationship arose because Defendant was entrusted with
4 Plaintiff and the Class's Personal Information.

5 112. Defendant breached its fiduciary duty that it owed Plaintiff and
6 the Class by failing to case in good faith, fairness, and honesty; by failing to act
7 with the highest and finest loyalty; and by failing to protect the Personal
8 Information of Plaintiff and the Class Members.

9 113. Defendant's breach of fiduciary duties was a legal cause of
10 damages to Plaintiff and the Class.

11 114. But for Defendant's breach of fiduciary duty, the damage to
12 Plaintiff and the Class would not have occurred, and the Data Breach contributed
13 substantially to producing the damage to Plaintiff and the Class.

14 115. As a direct and proximate result of Defendant's breach of
15 fiduciary duty, Plaintiff and the Class are entitled to actual, consequential, and
16 nominal damages and injunctive relief, with amounts to be determined at trial.

17 **FOURTH CAUSE OF ACTION**

18 **(Breach of Confidence – *By Plaintiff on behalf of the Class, against***
19 ***Defendant and Does 1-50)***

20 116. Plaintiff incorporates by reference all allegations of the
21 preceding paragraphs as though fully set forth herein.

22 117. Defendant was fully aware of the confidential nature of the
23 Personal Information of Plaintiff and Class Members that it was provided.

24 118. As alleged herein and above, Defendant's relationship with
25 Plaintiff and the Class was governed by promises and expectations that Plaintiff
26 and Class Members' Personal Information would be collected, stored, and protected
27 in confidence, and would not be accessed by, acquired by, appropriated by,
28

1 disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or
2 viewed by unauthorized third parties.

3 119. Plaintiff and Class members provided their respective Personal
4 Information to Defendant's clients, and by proxy to Defendant, with the explicit
5 and implicit understandings that Defendant would protect and not permit the
6 Personal Information to be accessed by, acquired by, appropriated by, disclosed to,
7 encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by
8 unauthorized third parties.

9 120. Plaintiff and Class Members provided their respective Personal
10 Information to Defendant's clients, and by proxy to Defendant, with the explicit
11 and implicit understandings that Defendant would take precautions to protect their
12 Personal Information from unauthorized access, acquisition, appropriation,
13 disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as
14 following basic principles of protecting their networks and data systems.

15 121. Defendant voluntarily received, in confidence, Plaintiff and
16 Class members' Personal Information with the understanding that the Personal
17 Information would not be accessed by, acquired by, appropriated by, disclosed to,
18 encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the
19 public or any unauthorized third parties.

20 122. Due to Defendant's failure to prevent, detect, and avoid the Data
21 Breach from occurring by, inter alia, not following best information security
22 practices to secure Plaintiff and Class Members' Personal Information, Plaintiff and
23 Class Members' Personal Information was accessed by, acquired by, appropriated
24 by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by,
25 and/or viewed by unauthorized third parties beyond Plaintiff and Class Members'
26 confidence, and without their express permission.

1 123. As a direct and proximate cause of Defendant's actions and/or
2 omissions, Plaintiff and Class members have suffered damages as alleged herein.

3 124. But for Defendant's failure to maintain and protect Plaintiff and
4 Class Members' Personal Information in violation of the parties' understanding of
5 confidence, their Personal Information would not have been accessed by, acquired
6 by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen
7 by, used by, and/or viewed by unauthorized third parties. Defendant's Data Breach
8 was the direct and legal cause of the misuse of Plaintiff and Class members'
9 Personal Information, as well as the resulting damages.

10 125. The injury and harm Plaintiff and Class Members suffered and
11 will continue to suffer was the reasonably foreseeable result of Defendant's
12 unauthorized misuse of Plaintiff and Class members' Personal Information.
13 Defendant knew its data systems and protocols for accepting and securing Plaintiff
14 and Class Members' Personal Information had security and other vulnerabilities
15 that placed Plaintiff and Class members' Personal Information in jeopardy.

16 126. As a direct and proximate result of Defendant's breaches of
17 confidence, Plaintiff and Class members have suffered and will suffer injury, as
18 alleged herein, including but not limited to (a) actual identity theft; (b) the
19 compromise, publication, and/or theft of their Personal Information; (c) out-of-
20 pocket expenses associated with the prevention, detection, and recovery from
21 identity theft and/or unauthorized use of their Personal Information; (d) lost
22 opportunity costs associated with effort expended and the loss of productivity
23 addressing and attempting to mitigate the actual and future consequences of the
24 Data Breach, including but not limited to efforts spent researching how to prevent,
25 detect, contest, and recover from identity theft; (e) the continued risk to their
26 Personal Information, which remains in Defendant's possession and is subject to
27 further unauthorized disclosures so long as Defendant fail to undertake appropriate
28

1 and adequate measures to protect Class Members' Personal Information in their
2 continued possession; (f) future costs in terms of time, effort, and money that will
3 be expended as result of the Data Breach for the remainder of the lives of Plaintiff
4 and Class Members; and (g) the diminished value of Plaintiff and Class Members'
5 Personal Information.

6 **FIFTH CAUSE OF ACTION**

7 ***(Invasion of Privacy – By Plaintiff on behalf of the Class, against***
8 ***Defendant and Does 1-50)***

9 127. Plaintiff incorporates by reference all allegations of the
10 preceding paragraphs as though fully set forth herein.

11 128. Plaintiff and Class Members had a legitimate expectation of
12 privacy regarding their Personal Information and were accordingly entitled to the
13 protection of this information against disclosure to unauthorized third parties.

14 129. Defendant owed a duty to Plaintiff and Class Member to keep
15 their Personal Information confidential.

16 130. Defendant affirmatively and recklessly disclosed Plaintiff and
17 Class Members' Personal Information to unauthorized third parties.

18 131. The unauthorized disclosure and/or acquisition (i.e., theft) by a
19 third party of Plaintiff and Class Members' Personal Information is highly
20 offensive to a reasonable person.

21 132. Defendant's reckless and negligent failure to protect Plaintiff and
22 Class Members' Personal Information constitutes an intentional interference with
23 Plaintiff and the Class Members' interest in solitude or seclusion, either as to their
24 person or as to their private affairs or concerns, of a kind that would be highly
25 offensive to a reasonable person.

133. In failing to protect Plaintiff and Class Members' Personal Information, Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

134. Because Defendant failed to properly safeguard Plaintiff and Class Members' Personal Information, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

135. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

136. As a proximate result of Defendant's acts and omissions, Plaintiff and the Class Members' private and sensitive Personal Information was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

137. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Personal Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

138. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiff and the Class's Personal Information.

139. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff and Class Members' Personal Information.

140. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring

1 of their credit history for identity theft and fraud, plus prejudgment interest, and
2 costs.

3 **SIXTH CAUSE OF ACTION**

4 **(Injunctive Relief/Declaratory Relief – *By Plaintiff on behalf of the***
5 ***Class, against Defendant and Does 1-50)***

6 141. Plaintiff incorporates by reference all allegations of the
7 preceding paragraphs as though fully set forth herein.

8 142. Plaintiff and members of the Class entered into an implied
9 contract that required Defendant to provide adequate security for the Personal
10 Information it collected from Plaintiff and the Class.

11 143. Defendant owe a duty of care to Plaintiff and the members of the
12 Class that requires them to adequately secure Personal Information.

13 144. Defendant still possess Personal Information regarding Plaintiff
14 and members of the Class.

15 145. Since the Data Breach, Defendant has announced few if any
16 changes to their data security infrastructure, processes or procedures to fix the
17 vulnerabilities in their computer systems and/or security practices which permitted
18 the Data Breach to occur and go undetected for months and, thereby, prevent
19 further attacks.

20 146. Defendant has not satisfied its contractual obligations and legal
21 duties to Plaintiff and the Class. In fact, now that Defendant's insufficient
22 information security is known to hackers, the Personal Information in Defendant
23 possession is even more vulnerable to cyberattack.

24 147. Actual harm has arisen in the wake of the Data Breach regarding
25 Defendant's contractual obligations and duties of care to provide security
26 measures to Plaintiff and the members of the Class. Further, Plaintiff and the
27 members of the Class are at risk of additional or further harm due to the exposure
28

1 of their Personal Information and Defendant's failure to address the security
2 failings that lead to such exposure.

3 148. There is no reason to believe that Defendant's security measures
4 are any more adequate now than they were before the breach to meet Defendant's
5 contractual obligations and legal duties.

6 149. Plaintiff, therefore, seeks a declaration (1) that Defendant's
7 existing security measures do not comply with their contractual obligations and
8 duties of care to provide adequate security, and (2) that to comply with their
9 contractual obligations and duties of care, Defendant must implement and maintain
10 reasonable security measures, including, but not limited to:

- 11 xix. Ordering that Defendant engage third-party security
12 auditors/penetration testers as well as internal security personnel
13 to conduct testing, including simulated attacks, penetration tests,
14 and audits on Defendant's systems on a periodic basis, and
15 ordering Defendant to promptly correct any problems or issues
16 detected by such third-party security auditors;
- 17 xx. Ordering that Defendant engage third-party security auditors and
18 internal personnel to run automated security monitoring;
- 19 xxi. Ordering that Defendant audit, test, and train their security
20 personnel regarding any new or modified procedures;
- 21 xxii. Ordering that Defendant's segment customer data by, among
22 other things, creating firewalls and access controls so that if one
23 area of Defendant's systems is compromised, hackers cannot
24 gain access to other portions of Defendant's systems;
- 25 xxiii. Ordering that Defendant purge, delete, and destroy in a
26 reasonably secure manner customer data not necessary for its
27 provisions of services;

- 1 xxiv. Ordering that Defendant conduct regular database scanning and
2 securing checks or require as such from any third-party source
3 where such information is retained;
- 4 xxv. Ordering that Defendant routinely and continually conduct
5 internal training and education to inform internal security
6 personnel how to identify and contain a breach when it occurs
7 and what to do in response to a breach; and
- 8 xxvi. Ordering Defendant to meaningfully educate its current, former,
9 and prospective employees and subcontractors about the threats
10 they face as a result of the loss of their financial and personal
11 information to third parties, as well as the steps they must take to
12 protect themselves.

13
14 **PRAYER FOR RELIEF**

15 WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as
16 follows:

- 17 a. An order certifying this action as a class action under Fed. R. Civ. P.
18 23, defining the Class as requested herein, appointing the undersigned
19 as Class counsel, and finding that Plaintiff are proper representatives of
20 the Class requested herein;
- 21 b. A judgment in favor of Plaintiff and the Class awarding them
22 appropriate monetary relief, including actual and statutory damages,
23 punitive damages, attorney fees, expenses, costs, and such other and
24 further relief as is just and proper.
- 25 c. An order providing injunctive and other equitable relief as necessary to
26 protect the interests of the Class as requested herein;
- 27
28

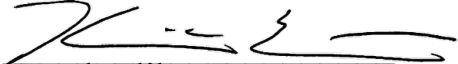
- 1 d. An order requiring Defendant to pay the costs involved in notifying the
2 Class members about the judgment and administering the claims
3 process;
4 e. A judgment in favor of Plaintiff and the Class awarding them pre-
5 judgment and post-judgment interest, reasonable attorneys' fees, costs
6 and expenses as allowable by law; and
7 f. An award of such other and further relief as this Court may deem just
8 and proper.
9

10 **DEMAND FOR JURY TRIAL**

11 Plaintiff hereby demands a trial by jury on all appropriate issues raised in this
12 Complaint.
13
14

15 Dated: 08/13/2024

EMPLOYEE JUSTICE LEGAL GROUP P.C.

16
17 By: 
18 Kaveh Elihu, Esq.
19 Saima Ali Gipson, Esq.
20 *Attorney for Plaintiff and Proposed*
21 *Counsel for the Classes*
22
23
24
25
26
27
28